PCT/DE 2004/001299

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 28 208.4

Anmeldetag: 24. Juni 2003

Anmelder/Inhaber: ROBERT BOSCH GMBH, 70469 Stuttgart/DE

Bezeichnung: Verfahren zur Umschaltung zwischen wenigstens zwei Betriebsmodi einer Prozessoreinheit sowie entsprechende Prozessoreinheit

IPC: G 06 F 9/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 16. Juli 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Letang

A 9161
08/00
EDV-L

R. 306264

20.06.03 Sy/Ho

ROBERT BOSCH GMBH, 70442 Stuttgart

Verfahren zur Umschaltung zwischen wenigstens zwei Betriebsmodi einer Prozessoreinheit sowie entsprechende Prozessoreinheit

Stand der Technik

Die Erfindung geht aus von einem Verfahren zur Umschaltung zwischen wenigstens zwei Betriebsmodi einer Prozessoreinheit sowie einer entsprechenden Prozessoreinheit mit wenigstens zwei integrierten Ausführungseinheiten gemäß den Oberbegriffen der unabhängigen Ansprüche.

Solche Prozessoreinheiten mit wenigstens zwei integrierten Ausführungseinheiten sind auch als Dual-Core- oder Multi-Core-Architekturen bekannt. Solche Dual-Core- oder Multi-Core-Architekturen werden nach heutigem Stand der Technik hauptsächlich aus zwei Gründen vorgeschlagen:

Zum Einen kann damit eine Leistungssteigerung, also eine Performance-Steigerung erreicht werden, indem die beiden Ausführungseinheiten oder Cores als zwei Recheneinheiten auf einem Halbleiterbaustein betrachtet und behandelt werden. In dieser Konfiguration bearbeiten die zwei Ausführungseinheiten oder Cores unterschiedliche Programme respektive Tasks. Dadurch lässt sich eine Leistungssteigerung erzielen, weshalb diese Konfiguration als Leistungsmodus oder Performance-Mode bezeichnet wird.

Der zweite Grund, eine Dual-Core- oder Multi-Core-Architektur zu realisieren, ist eine Sicherheitssteigerung, indem die beiden Ausführungseinheiten redundant das gleiche

Programm abarbeiten. Die Ergebnisse der beiden Ausführungseinheiten oder CPUs, also Cores werden verglichen und ein Fehler kann bei dem Vergleich auf Übereinstimmung erkannt werden. Im Folgenden wird diese Konfiguration als Sicherheitsmodus oder Safety-Mode bezeichnet.

Im Allgemeinen sind die beiden genannten Konfigurationen exklusiv auf der Dual- oder Multi-Core-Architektur enthalten, d. h. der Rechner mit den wenigstens zwei Ausführungseinheiten, wird prinzipiell nur in einem Modus betrieben, dem Performance-Modus oder dem Safety-Modus.

Aufgabe der Erfindung ist es, einen kombinierten Betrieb einer solchen Dual- oder Multi-Core-Prozessoreinheit bezüglich wenigstens zweier Betriebsarten zu ermöglichen und dabei eine optimierte Umschaltstrategie, insbesondere zwischen einem Sicherheitsmodus zur Sicherheitssteigerung und einem Leistungsmodus zur Leistungssteigerung zu erzielen.

Vorteile der Erfindung

Es ist zum Einen aus Sicherheitsgründen eine redundante Ausführung der Programme respektive Tasks erwünscht, andererseits ist aus Kostengründen das Bereithalten von redundanter Hardware bei der Ausführung der nicht sicherheitskritischen Funktionen nicht erstrebenswert. Dieser Zielkonflikt wird erfindungsgemäß durch eine optimierte Umschaltung zwischen wenigstens zwei Betriebsmodi und einer Prozessoreinheit gelöst. So geht die Erfindung von einem Verfahren zur Umschaltung zwischen wenigstens zwei Betriebsmodi, einer Prozessoreinheit mit wenigstens zwei Ausführungseinheiten sowie entsprechender Prozessoreinheit aus.

Vorteilhafter Weise wird die Umschaltung von einem ersten in einen zweiten Betriebsmodus dadurch realisiert, dass auf eine vorgegebene, als Umschalttrigger wirkende Speicheradresse zugegriffen wird. D. h. es werden Hardwarekomponenten wie Umschaltmittel (Mode Selektor) oder Vergleichsmittel und ein entsprechendes Verfahren vorgestellt, wie im Betrieb zwischen sicherheitskritischen Programmen, welche also im Sicherheitsmodus redundant ausgeführt werden und nicht sicherheitskritischen

Programmen, welche im Leistungsmodus unabhängig voneinander auf beiden Ausführungseinheiten ausgeführt werden, optimal umgeschaltet werden kann.

Dabei werden die gleichen Programme im ersten Betriebsmodus durch die wenigstens zwei Ausführungseinheiten synchron abgearbeitet und durch vorgesehene Vergleichsmittel dahingehend überprüft, dass die bei der Abarbeitung der gleichen Programme entstehenden Zustände der Ausführungseinheiten übereinstimmen. Bei Abweichungen diesbezüglich sind dann verschiedene Fehlerreaktionen von einer Fehleranzeige über einen Notbetrieb bis hin zur Abschaltung der fehlerhaften Einheit denkbar.

In einer speziellen Ausführungsform entspricht dem ersten Betriebsmodus und dem zweiten Betriebsmodus der Leistungsmodus. Eine Umschaltung vom zweiten Betriebsmodus in den ersten Betriebsmodus erfolgt dabei zweckmäßiger Weise durch eine Unterbrechungsanforderung, insbesondere ausgelöst durch ein Unterbrechungsmittel, wobei die Unterbrechungsanforderung einerseits durch eine Zeitbedingung auslösbar ist oder auch durch eine Zustandsbedingung, also einem bestimmten Zustand wenigstens einer der beiden Ausführungseinheiten oder auch dem Auftreten eines bestimmten Ereignisses entspricht.

Vorteilhafter Weise erfolgt eine spezielle Aufteilung in wenigstens drei getrennte Speicherbereiche, wobei die Ausführungseinheiten abhängig vom jeweiligen Betriebsmodus auf einen ersten Speicherbereich oder einen zweiten Speicherbereich Zugriff haben, respektive mit diesem in Verbindung stehen. Dabei ist zweckmäßiger Weise in einer speziellen Ausführungsform jeder der wenigstens zwei Ausführungseinheiten jeweils ein erster Speicherbereich auf der Prozessoreinheit zugeordnet, mit welchen diese im ersten Betriebsmodus, also insbesondere dem Sicherheitsmodus, in Verbindung stehen bzw. darauf zugreifen. Im zweiten Betriebsmodus haben beide Ausführungseinheiten nur auf einen, beiden Ausführungseinheiten zugeordneten zweiten Speicherbereich Zugriff bzw. stehen mit diesem in Verbindung.

Zweckmäßiger Weise sind nun Überwachungsmittel, insbesondere die Umschaltmittel selber derart vorgesehen, dass überwacht wird, dass im jeweiligen Betriebsmodus nur auf

die entsprechenden Speicherbereiche zugegriffen wird bzw. die entsprechende Verbindung zu den Speicherbereichen besteht. D. h. im zweiten Betriebsmodus greifen die Auswertemittel nur auf den zweiten Speicherbereich zu und nicht auf die ersten Speicherbereiche, und im ersten Betriebsmodus erfolgt der Zugriff nur auf die jeweiligen ersten Speicherbereiche, und nicht auf den zweiten Speicherbereich, was durch vorgenannte Überwachungsmittel überprüft und in eventuell entsprechende Fehlerreaktionen wie Fehlermeldung, Notbetrieb oder Abschaltung sanktioniert wird.

Dabei ist jeder der genannten drei Speicherbereiche, also die wenigstens zwei ersten Speicherbereiche sowie der zweite Speicherbereich in einem getrennten Speicherbaustein vorgesehen, so dass wenigstens drei Speicherbausteine auf der Prozessoreinheit zur Verfügung stehen. Dabei sind zweckmäßiger Weise die sicherheitskritischen Programme jeweils in einem ersten Speicherbereich, und die nicht sicherheitskritischen Programme im zweiten Speicherbereich abgelegt, wobei zweckmäßiger Weise die vorgegebene Speicheradresse, welche die genannte Triggerfunktion bezüglich der Umschaltung aufweist, in dem zweiten Speicherbereich enthalten ist.

Ein weiterer Vorteil ergibt sich, wenn für den Vergleich der Zustände der Ausführungseinheiten im ersten Betriebsmodus explizite Vergleichsmittel auf der Prozessoreinheit vorgesehen sind und diese Vergleichsmittel nur im ersten Betriebsmodus in Funktion sind und beim Übergang in den zweiten Betriebsmodus außer Funktion gesetzt werden, so dass im nichtredundanten, nicht sicherheitskritischen Betrieb kein Vergleich und damit keine unter Umständen provozierte Fehlerreaktion erfolgt.

Weitere Vorteile und vorteilhafte Ausgestaltungen ergeben sich aus den Merkmalen der Ansprüche sowie den Inhalten von Beschreibung und Zeichnung.

Zeichnung

Die Erfindung wird nachfolgend anhand der in der Zeichnung dargestellten Figuren näher erläutert. Dabei zeigt

Figur 1 eine erfindungsgemäße Prozessoreinheit mit wenigstens zwei Ausführungseinheiten und den erfindungsgemäßen Hardwarekomponenten.

Figur 2 offenbart eine Umschaltung vom Sicherheitsmodus in den Leistungsmodus, wohingegen

Figur 3 eine Umschaltung vom Leistungsmodus in den Sicherheitsmodus darstellt.

Beschreibung der Ausführungsbeispiele

In Steuerungsanwendungen, insbesondere auf dem Gebiet der Kraftfahrzeugsteuerung, wie Motorsteuerung, Bremsensteuerung oder auch Lenkung und Getriebe usw., aber ebenso in Industrieanwendungen wie der Automatisierung oder im Werkzeugmaschinenbereich gibt es im Allgemeinen Softwaretasks oder Programme, die eine redundante Ausführung aus Sicherheitsgründen erfordern, um das Auftreten von Fehlern zu erkennen. Solche sicherheitskritischen Anwendungen weisen aber neben diesen sicherheitskritischen Programmen auch Softwarebestandteile oder Programme auf, die auch fehlerhaft sein dürfen, da sie nicht für das Erbringen der sicherheitskritischen Funktion selbst nötig sind bzw. damit befasst sind, sondern nur eine zusätzliche Funktion, insbesondere eine Komfortfunktion erbringen. Aus Sicherheitsgründen ist eine redundante Ausführung erwünscht, aus Kostengründen das Bereithalten von redundanter Hardware nicht erstrebenswert. Erfindungsgemäß wird diese Problemstellung durch das optimierte Umschalten zwischen wenigstens zwei Betriebsmodi, der Prozessoreinheit, wie bereits in den Vorteilen beschrieben und nachfolgend näher erläutert, gelöst.

Somit wird im Folgenden der Einsatz der Erfindung in einem sicherheitskritischen System, beispielsweise einem fahrzeugimmanenten System wie Bremse, Lenkung, Getriebe oder Motor dargestellt. Die erfindungsgemäße Prozessoreinheit des Systems besteht dabei aus einer Dual-Core-Architektur entsprechend Figur 1, also einer Prozessoreinheit 100 mit wenigstens zwei Ausführungseinheiten 101 und 102 (CPU1 und CPU2). Den beiden Ausführungseinheiten 101, 102, also CPU1 und CPU2 sind in diesem Beispiel jeweils ein Arbeitsspeicher 110 bzw. 111 zugeordnet, auch als RAM1 und RAM2 bezeichnet. Beide Ausführungseinheiten 101 und 102 sind mit einem Vergleichsmittel, einem Vergleicher 170 verbunden. Jede Ausführungseinheit hat weiterhin eine Verbindung zu einem Umschaltmittel, einem Mode-Selektor 130 bzw. 131, mit welchem auch der Vergleichsbaustein, das Vergleichsmittel 170 Verbindungen

aufweist. Über jeweils einen Bus 140 bzw. 141 ist der jeweils flüchtige Arbeitsspeicher 110 bzw. 111 sowie die Umschaltmittel 130 und 131 mit jeweils einem ersten Speichermittel 150 bzw. 151 sowie einem zweiten Speichermittel 180 verbunden.

In diesem Ausführungsbeispiel werden zwei Betriebssysteme verwendet, eines für die sicherheitskritischen Programme oder Tasks und eines für die nicht sicherheitskritischen Programme oder Tasks. Als Betriebssystem für die sicherheitskritischen Programme wird beispielsweise OSEKtime OS, und als Betriebssystem für die nicht sicherheitskritischen Tasks beispielsweise OSEK OS verwendet.

Die Anwendungssoftware ist, wie bereits erwähnt, aufgeteilt in sicherheitskritische Programme und nicht sicherheitskritische Programme. Alle Programme oder Tasks, die als nicht sicherheitskritisch eingestuft sind, dürfen versagen, fehlerhaft ausgeführt oder überhaupt nicht ausgeführt werden. Eine Gefährdung des Gesamtsystems bzw. der Umgebung ist dadurch nicht möglich. Der sichere Betrieb des Gesamtsystems wird alleine durch die als sicherheitskritisch eingestuften Programme respektive Tasks möglich. Allerdings besteht die Möglichkeit, dass der Betrieb, sofern er alleine durch die sicherheitskritischen Tasks bzw. Programme durchgeführt wird, zu einem Qualitätsverlust bzw. der Gesamtfunktion führt, die allerdings innerhalb vorgebbarer Toleranzen als tolerierbar eingestuft wurde.

Die sicherheitsrelevanten, also die sicherheitskritischen Tasks oder Programme werden redundant auf beiden Ausführungseinheiten 101 und 102, also beiden CPUs, CPU1 und CPU2 ausgeführt. Dabei werden diese Programme unter der Kontrolle des ersten Betriebssystems, hier OSEKtime OS abgearbeitet. Dazu ist der in Figur 1 dargestellte nicht flüchtige Speicherbereich 150 bzw. 151 in zwei Teile verdoppelt, so dass entsprechend zweier Ausführungseinheiten zwei erste Speicherbereiche 150 und 151 vorliegen. In diesen ersten Speicherbereichen liegen die sicherheitskritischen Programme respektive Tasks verdoppelt, also redundant. D. h. jede der sicherheitskritischen Tasks ist zum Einen im Speicherbereich 150 und zum Anderen im Speicherbereich 151 lokalisiert. Dabei kann insbesondere das erste Betriebssystem selbst als sicherheitskritisch eingestuft werden und wird somit ebenfalls in beiden Speicherbereichen abgelegt. D. h. in unserem Beispiel, dass das Betriebssystem OSEKtime OS zum Einen im Speicherbereich 150 und zum Anderen im Speicherbereich 151 jeweils abgelegt ist. Dabei sind die beiden ersten

Speicherbereiche in einer besonderen Ausführung jeweils als eigener nicht flüchtiger Speicherbaustein ROM1 bzw. ROM2 ausgeführt, welche als ROM, PROM, EPROM, EEPROM, Flash-EPROM usw. ausgeführt werden können.

Dabei ist nicht zwingend eine Doppelablage der sicherheitskritrischen Programme oder Tasks erforderlich. Diese können auch durch Einsatz eines ECC-Codes (Error Code and Correction) abgesichert sein. Solche Methoden zur Fehlererkennung bei einem Speicher sind vielfältig, wobei die Grundvoraussetzung die Absicherung mit einem Fehlererkennungs- bzw. Fehlerkorrekturcode, also einer Signatur darstellt. Im einfachsten Fall kann diese Signatur nur aus einem Signaturbit, beispielsweise einem Paritybit bestehen. Andererseits kann die Absicherung auch durch komplexere ED-Codes (Error Detection) wie einen Berger-Code oder einen Bose-Lin-Code usw., oder auch durch einen komplexeren ECC-Code wie beispielsweise einen Hamming-Code, usw. realisiert werden, um durch entsprechende Bitzahl eine sicherere Fehlererkennung zu ermöglichen. Es kann aber auch als Codegenerator, beispielsweise eine Generatortabelle (fest verdrahtet oder in Software) verwendet werden, um bestimmten Eingangsmustern der Bits im Rahmen der Adresse ein gewünschtes Codemuster beliebiger Länge zuzuordnen. Damit kann, insbesondere durch die Korrekturfunktion die Datensicherheit im Speicher gewährleistet werden und eine Doppelablage vermieden werden. Dennoch erfolgt eine redundante Abarbeitung der sicherheitskritischen Programme in den beiden Ausführungseinheiten, wodurch Fehler in den Cores, also den Ausführungseinheiten durch Vergleich auf Übereinstimmung erfindungsgemäß aufgedeckt werden, wobei für diesen Fall der Erfindung entgegen Figur 1 nur ein erster Speicherbereich notwendig ist.

Die nicht sicherheitsrelevanten bzw. sicherheitskritischen Programme oder Tasks werden zur Leistungserhöhung auf beiden Ausführungseinheiten, also CPUs verteilt berechnet und unter der Kontrolle des jeweiligen Subbetriebsystems, also hier des OSEK-Subsystems ausgeführt. Insbesondere läuft somit auf jede der beiden Ausführungseinheiten ein unabhängiges Betriebssystem, hier ein unabhängiges OSEK-System. Der zweite Speicherbereich 180, in dem sich die nicht sicherheitskritischen Programme bzw. Tasks befinden, ist einfach vorhanden. Er wird von beiden Ausführungseinheiten 101 bzw. 102 benützt bzw. es wird von beiden auf ihn zugegriffen. Auch dieser zweite Speicherbereich kann in einer besonderen Ausführungsform als

eigener nicht flüchtiger Speicherbaustein ROM3 ausgebildet sein und als ROM, PROM, EPROM, EEPROM, Flash-EPROM usw. ausgestaltet werden.

Dabei können die Speicherbereiche, also die ersten und zweiten Speicherbereiche so ausgebildet sein, dass die ersten Speicherbereiche bzw. der erste Speicherbereich (bei ECC Absicherung) beispielsweise zwischen 0 und X bezogen auf die Adressen und der zweite Speicherbereich von X + 1 bis Y ebenfalls bezogen auf die Adressen ausgebildet sind. Im weiteren wird von einem verdoppelten ersten Speicherbereich ausgegangen, wobei wie vorher erläutert auch nur ein einzelner erster abgesicherter Speicherbereich Einsatz finden kann. Dann ist, wie schon gesagt, der erste Speicherbereich von 0 bis X doppelt eben jeweils in einem ersten Speicherbereich vorhanden. Dabei ist jeder erste Speicherbereich einer Ausführungseinheit konkret zugeordnet.

Im ersten Betriebsmodus, hier im Beispiel dem Sicherheitsmodus, laufen auf beiden Ausführungseinheiten, also beiden CPUs 101 und 102 redundant und insbesondere synchron die sicherheitskritischen Programme bzw. Tasks ab. Im Vergleichsmittel, dem Vergleicher 170, werden die jeweiligen CPU-Zustände miteinander verglichen. Dabei können bestimmten Programmphasen bestimmte Zustände zugeordnet sein, die dann zeitunkritisch, also zu einem beliebigen Zeitpunkt verglichen werden können, sofern diese zwischengespeichert und beispielsweise durch eine Kennung eindeutig zuordenbar sind, verglichen werden können. Im bevorzugten Fall aber werden die sicherheitskritischen Programme respektive Tasks nicht nur redundant, sondern synchron abgearbeitet, so dass im Betrieb direkt ein Vergleich der jeweiligen Zustände der Ausführungseinheiten durchgeführt werden kann. Die neuen Befehle und/oder Daten werden dann entsprechend aus dem jeweilig zugeordneten ersten Speicherbereich 150 respektive 151 geladen und abgearbeitet. Im Vergleicher 170 werden die CPU-Zustände auf Übereinstimmung geprüft, wobei bei einer Abweichung der Zustände, die sich entsprechen sollten, auf Fehler erkannt wird. Als Fehlerreaktion ist zum Einen eine Fehleranzeige bezüglich des jeweiligen Systems, in dem die Prozessoreinheit verbaut ist, möglich und zum Anderen Fehlerreaktionen wie ein Notbetrieb, also das Betreiben des Systems, dem die Prozessoreinheit innewohnt, in einem abgesicherten Notbetrieb, beispielsweise mit extra dafür vorgesehenen Programmen und/oder Daten. Dabei kann auch bei einer weitergehenden Fehlerauswertung, z. B. einem n- aus m-Test, wobei n und m natürliche Zahlen sind und $n > 2$ sowie $m > n > n/2$ oder auch einem 1 aus k-Code,

wobei k einer natürlichen Zahl > 1 entspricht. Wird beispielsweise durch solch einen Test eindeutig eine Ausführungseinheit als fehlerhaft erkannt, kann als weitere Fehlerreaktion auch ein Abschalten dieser Ausführungseinheit und Notbetrieb der verbliebenen Einheit oder ein Umschalten der fehlerhaften Ausführungseinheit in den Notbetrieb erfolgen.

Im Safety-Mode, also dem Sicherheitsmodus oder allgemeiner dem ersten Betriebsmodus, ist ein Zugriff der Ausführungseinheiten nur auf Adressen bzw. Daten in den ersten Speicherbereichen zulässig. D. h. die jeweilige Ausführungseinheit darf im ersten Betriebsmodus nur auf den, insbesondere ihr zugeordneten, ersten Speicherbereich zugreifen. Dies wird durch Überwachungsmittel, insbesondere die Umschaltmittel oder Mode-Selektoren 130 respektive 131 bzw. Überwachungsmittel in den Mode-Selektoren 130 und 131 überprüft. Treten hierbei Fehler auf, ist eine vergleichbare Fehlerreaktion, wie oben beschrieben, bezüglich eines Vergleichfehlers bei Übereinstimmung der CPU-Zustände denkbar und vorsehbar. D. h. aber auch, dass die Umschaltmittel, also hier die Mode-Selektoren 130 respektive 131 für diesen Fall des ersten Betriebsmodus eine Verbindung in den jeweils zugehörigen ersten Speicherbereich 150 respektive 151 via Bus 140 respektive 141 herstellen bzw. eine entsprechende Zugriffsverletzung überwachen.

Im zweiten Betriebsmodus dieses Ausführungsbeispiels werden die nicht sicherheitskritischen Programme respektive Tasks abgearbeitet. Auf beiden Ausführungseinheiten, also den CPUs 1 und 2 (101, 102) laufen verschiedene nicht sicherheitskritische Programme. Dazu gehört beispielsweise auch das Betriebssystem selbst für den zweiten Betriebsmodus, also das OSEK-Subsystem. Die beiden Ausführungseinheiten oder CPUs teilen sich damit einen nicht flüchtigen zweiten Speicherbereich, der, wie vorher beschrieben, ausgebildet sein kann. Allerdings ist jedem CPU ein eigener flüchtiger Arbeitsspeicherbereich RAM1 und RAM2, 110 respektive 111 zugeordnet. Da entsprechende solche nicht sicherheitskritische Programme nicht oder nicht alle doppelt ausgeführt sind, besteht zumindest theoretisch die Möglichkeit, dass sich beide Ausführungseinheiten gegenseitig durch Warten auf Freigabe einer Ressource blockieren. Dem ist durch geeignete Verteilung der Tasks bzw. Programme, beispielsweise nach einem Schedule auf die Ausführungseinheiten 101 und 102 entgegenzuwirken. Dabei sind auch weitere Maßnahmen wie beispielsweise ein abwechselnder Zugriff oder ein abhängig vom jeweiligen Programm priorisierter Zugriff

usw. möglich. In diesem zweiten Betriebsmodus, dem Leistungsmodus gemäß unserem Ausführungsbeispiel ist kein Zugriff auf eine Adresse im ersten Speicherbereich zulässig. Auch hier erfolgt die Überprüfung durch Überprüfungsmittel, insbesondere durch die Umschaltmittel, die Mode-Selektoren, oder aber die Überprüfungsmittel sind in den Mode-Selektoren separat ausgeführt. Bei einem erkannten fehlerhaften Zugriff im zweiten Betriebsmodus kann auch hier eine entsprechende Fehlerreaktion eingeleitet werden. Dabei ist zum Einen eine Fehlerreaktion entsprechend des ersten Betriebsmodus denkbar und vorgebbar. Dies ist insbesondere dadurch sinnvoll, da bei einem fehlerhaften Zugriff unter Umständen ja auf sicherheitskritische Speicherbereiche zugegriffen wird. Zum Einen ist dies dadurch realisierbar, dass eine Verbindung zum zweiten Speicherbereich nur im zweiten Betriebsmodus aufgebaut wird und die Verbindung zu den ersten Speicherbereichen in diesen Betriebsmodus gekappt wird oder der Zugriff auf den ersten Speicherbereich anderweitig verhindert und nur in den zweiten Speicherbereich erlaubt wird.

Das Umschalten zwischen den Betriebsmodi ist nun ausführlich in den Figuren 2 und 3 nochmals beschrieben.

Um von dem ersten Betriebsmodus, also hier dem Sicherheitsmodus oder Safety-Mode in den zweiten Betriebsmodus, also hier Leistungsmodus oder Performance-Mode zu gelangen, ist ein Zugriff auf eine vorgegebene bzw. ausgezeichnete Adresse erforderlich, wodurch ein Wechsel in den zweiten Betriebsmodus erfolgt. Diese ausgezeichnete Adresse kann dabei im ersten Speicherbereich bei der Programmabarbeitung auftreten bzw. entsprechend von Außen zugeführt werden. D. h. im ersten Betriebsmodus oder Sicherheitsmodus darf lediglich auf Adressen bzw. auf ein Programm im ersten Speicherbereich zugegriffen werden; falls in diesem Sicherheitsmodus auf eine andere Adresse z.B. im zweiten Speicherbereich zugegriffen wird, liegt ein Fehler mit möglicher entsprechender Fehlerreaktion, wie oben beschrieben, vor. In Figur 2 ist dies noch einmal verdeutlicht. Im Block 200 sind beide Ausführungseinheiten 101 und 102 im ersten Betriebsmodus, also dem Sicherheitsmodus. In Abfrage 210 wird überprüft, ob die Adresse des nächsten Befehls gleich der Triggeradresse der entsprechenden ausgezeichneten Umschaltadresse ist. Ist dies nicht der Fall, sind beide Verarbeitungseinheiten weiterhin im ersten Betriebsmodus und greifen somit jeweils auf die ersten Speicherbereiche 150, 151 zu. Entspricht allerdings die Adresse des nächsten

Befehls und/oder Datums der Triggeradresse, so erfolgt im Block 220 die Umschaltung bzw. der Wechsel in den zweiten Betriebsmodus, den Leistungs- oder Performance-Mode. Jede Ausführungseinheit erhält dabei außerdem eine Adresse im zweiten Speicherbereich, bei welcher die Abarbeitung im zweiten Betriebsmodus fortzusetzen ist. Dabei wird die Vergleichseinheit bzw. das Vergleichsmittel 170 abgeschalten, also außer Funktion gesetzt (disabled). Im Block 230 ist somit die erste Verarbeitungseinheit 101 im zweiten Betriebsmodus und im Block 231 die zweite Ausführungseinheit 102 ebenfalls im zweiten Betriebsmodus, dem Performance-Mode. D. h. die einzige Möglichkeit, um vom Sicherheitsmodus, dem Safety-Mode in den Performance-Mode zu gelangen, ist im konkreten Beispiel beispielsweise ein Aufruf einer speziellen OSEKtime-Task $T_{Trigger}$ wie z.B. der ttidle Task des OSEKtime Betriebssystems, respektive einer darin enthaltenen, als Trigger-Adresse ausgezeichneten Adresse, insbesondere der Anfangsadresse dieses Programmteils bzw. dieser Task. Insbesondere wenn die beiden Ausführungseinheiten synchron arbeiten, geschieht dieser Aufruf in beiden CPUs notwendigerweise gleichzeitig. Die $T_{Trigger}$-Task wie eben ttidle ist dabei z.B. ein Aufruf des OSEK-Schedulers, welcher im zweiten Speicherbereich 180 liegt. Beispielsweise in den Umschalteinrichtungen, also den Mode-Selektoren 130, 131 ist diese entsprechende Adresse als Triggeradresse eingestellt, um in den Leistungsmodus zu wechseln. Dies wird wie gesagt im Block 210, also eben den Mode-Selektoren, den Umschaltmitteln geprüft. Damit dürfen zukünftige Adresszugriffe eben bis zu einem erneuten Wechsel in den Sicherheitsmodus nur noch in den ROM-Bereich 180, also den nicht flüchtigen zweiten Speicherbereich erfolgen.

In Figur 3 ist nun die Umschaltung bzw. der Wechsel vom Leistungsmodus, also dem Performance-Mode insbesondere zurück in den ersten Betriebsmodus, den Sicherheitsmodus oder Safety-Mode dargestellt. In Block 300 ist Ausführungseinheit 101, also CPU 1 im zweiten Betriebsmodus, dem Performance-Mode. Ebenso ist in Block 310 die zweite Ausführungseinheit 102 in eben diesem Leistungsmodus, diesem zweiten Betriebsmodus dieses Ausführungsbeispiels. In Block 320 bzw. Block 321 wird nun für jede Ausführungseinheit eine Unterbrechungsanforderung, ein Interrupt ausgelöst, durch welchen eine Umschaltung in Block 330 von beiden Ausführungseinheiten 101 und 102 in den ersten Betriebsmodus, den Sicherheitsmodus, erfolgt. Dabei wird das Vergleichsmittel der Vergleicher 170 wieder eingeschalten, und in Block 340 laufen dann beide Ausführungseinheiten wieder im Sicherheitsmodus, dem ersten Betriebsmodus. Die

Unterbrechungsanforderung kann dabei zum Einen durch eine Zeitbedingung, also einen Timerinterrupt ausgelöst werden oder durch eine Zustands- respektive Ereignisbedingung ausgelöst sein. Das bedeutet, um vom Leistungsmodus in den Sicherheitsmodus zu wechseln, wird eine Unterbrechungsanforderung des ersten Betriebssystem OSEKtime generiert. Dieser Timerinterrupt des gegenüber dem OSEK-Betriebssystem höherprioren OSEKtime-Betriebssystems ist in beiden CPUs gleich programmiert, da auf beiden CPUs das gleiche OSEKtime-System läuft. Insbesondere bei synchron laufenden OSEKtime-Systemen geht der Interrupt, also die Unterbrechungsanforderung bei beiden CPUs gleichzeitig ein. Wie gesagt, hat damit definitionsgemäß der OSEKtime-Scheduler-Interrupt eine sehr hohe, insbesondere die höchste Priorität. Beide Unterbrechungsanforderungen werden bei Synchronität dementsprechend gleichzeitig ausgeführt. Wie bereits erwähnt, wird mit Ausführungen dieser Unterbrechungsanforderungen auch das Vergleichsmittel 170 ebenfalls wieder in Funktion gesetzt, also in den ersten Betriebszustand, den Sicherheitsmodus, umgeschaltet und die Ausführungseinheiten laufen insbesondere erneut redundant.

Neben dem bereits genannten Timer-Interrupt kann auch ein Zustands- oder Ereignisinterrupt eingesetzt werden, um den genannten Betriebsmoduswechsel vom zweiten in den ersten Betriebsmodus zu bewerkstelligen. Dabei kann ein bestimmter Zustand der Ausführungseinheiten beispielsweise einen hochprioren Interrupt auslösen, der dann für beide Ausführungseinheiten Gültigkeit hat. Dies kann beispielsweise ein durch die Abarbeitung der Programme im ROM 180 generierter Zustand in einer CPU sein, die eine solch hochpriore Unterbrechungsanforderung, die auch für die zweite CPU gilt, auslöst. Ebenso kann ein Ereignis, insbesondere auch ein von extern der Prozessoreinheit zugeführtes Ereignis einen solchen Interrupt und damit den Betriebsmoduswechsel auslösen. Bevorzugt ist die erste Variante mit dem Timerinterrupt, aber der Zustands- oder Ereignisinterrupt, wie beschrieben, ist ebenfalls denkbar und hiermit offenbart.

Damit ist entsprechend der Aufgabe eine optimierte Umschaltung zwischen zwei Betriebsmodi einer Prozessoreinheit mit zwei integrierten Ausführungseinheiten erfindungsgemäß dargestellt, wobei das konkrete Ausführungsbeispiel nicht begrenzend im Hinblick auf die Grundideen des erfindungsgemäßen Gegenstandes wirken kann.

20.06.2003 Sy/Ho

ROBERT BOSCH GMBH, 70442 Stuttgart

Ansprüche

1. Prozessoreinheit mit wenigstens zwei Ausführungseinheiten, wobei Umschaltmittel enthalten sind durch welche zwischen wenigstens zwei Betriebsmodi der Prozessoreinheit umgeschalten werden kann, dadurch gekennzeichnet, dass die Umschaltmittel derart ausgestaltet sind, dass ein Wechsel von einem ersten Betriebsmodus in einen zweiten Betriebsmodus dadurch ausgelöst wird, dass durch die Prozessoreinheit auf eine vorgegebene Speicheradresse zugegriffen wird.

2. Prozessoreinheit nach Anspruch 1, dadurch gekennzeichnet, dass der erste Betriebsmodus einem Sicherheitsmodus entspricht, bei dem die zwei Ausführungseinheiten gleiche Programme abarbeiten und Vergleichsmittel vorgesehen sind, welche die bei der Abarbeitung der gleichen Programme entstehenden Zustände der Ausführungseinheiten auf Übereinstimmung vergleichen.

3. Prozessoreinheit nach Anspruch 2, dadurch gekennzeichnet, dass die Ausführungseinheiten derart ausgebildet sind, dass diese im ersten Betriebsmodus die gleichen Programme synchron abarbeiten.

4. Prozessoreinheit nach Anspruch 1, mit wenigstens drei getrennten Speicherbereichen, wobei in dem ersten Betriebsmodus jede Ausführungseinheit jeweils mit einem jeder Ausführungseinheit zugeordneten ersten Speicherbereich in Verbindung steht.

5. Prozessoreinheit nach Anspruch 1, mit wenigstens zwei getrennten Speicherbereichen, wobei in dem zweiten Betriebsmodus beide Ausführungseinheiten nur mit einem, beiden Ausführungseinheiten zugeordneten zweiten Speicherbereich in Verbindung stehen.

6. Prozessoreinheit nach Anspruch 1 und 5, dadurch gekennzeichnet, dass die vorgegebene Speicheradresse auf die zugegriffen werden soll in dem zweiten Speicherbereich lokalisiert ist.

7. Prozessoreinheit nach Anspruch 1, mit wenigstens zwei getrennten Speicherbereichen, wobei in dem ersten Betriebsmodus beide Ausführungseinheiten nur mit einem, beiden Ausführungseinheiten zugeordneten ersten Speicherbereich in Verbindung stehen.

8. Prozessoreinheit nach Anspruch 1 und 7, dadurch gekennzeichnet, dass die vorgegebene Speicheradresse als Triggeradresse im ersten Speicherbereich enthalten ist und die folgende Adresse auf die zugegriffen werden soll in dem zweiten Speicherbereich enthalten ist.

9. Prozessoreinheit nach Anspruch 1 und 5, dadurch gekennzeichnet, dass Überwachungsmittel, insbesondere die Umschaltmittel, vorgesehen sind, welche derart zur Überwachung ausgebildet sind, dass die Auswertemittel im zweiten Betriebsmodus nur mit dem zweiten Speicherbereich in Verbindung stehen.

10. Prozessoreinheit nach Anspruch 1 und 4, dadurch gekennzeichnet, dass Überwachungsmittel, insbesondere die Umschaltmittel, vorgesehen sind, welche derart zur Überwachung ausgebildet sind, dass die Auswertemittel im ersten Betriebsmodus nur jeweils mit dem ersten Speicherbereich in Verbindung stehen.

11. Prozessoreinheit nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass jeder der Speicherbereiche in einem getrennten Speicherbaustein vorgesehen ist.

12. Prozessoreinheit nach Anspruch 2, dadurch gekennzeichnet, dass die Vergleichsmittel bei Übergang in den zweiten Betriebsmodus, der einem Leistungsmodus entspricht außer Funktion gesetzt werden und ein Vergleich der Zustände nur im ersten Betriebsmodus erfolgt.

13. Prozessoreinheit nach Anspruch 1, dadurch gekennzeichnet, dass Unterbrechungsmittel enthalten sind, welche derart ausgebildet sind, dass diese eine

Rückkehr in den ersten Betriebsmodus durch eine Unterbrechungsanforderung ermöglichen.

14. Prozessoreinheit nach Anspruch 11, dadurch gekennzeichnet, dass die Unterbrechungsanforderung durch eine Zeitbedingung ausgelöst wird.

15. Prozessoreinheit nach Anspruch 11, dadurch gekennzeichnet, dass die Unterbrechungsanforderung durch eine Zustandsbedingung ausgelöst wird.

16. Verfahren zur Umschaltung zwischen wenigstens zwei Betriebsmodi einer Prozessoreinheit mit wenigstens zwei Ausführungseinheiten dadurch gekennzeichnet, dass ein Wechsel von einem ersten Betriebsmodus in einen zweiten Betriebsmodus dadurch ausgelöst wird, dass durch die Prozessoreinheit auf eine vorgegebene Speicheradresse zugegriffen wird.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass die Ausführungseinheiten im ersten Betriebsmodus die gleichen Programme synchron abarbeiten.

18. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass in beiden Betriebsmodi verschiedene Programme abgearbeitet werden, wobei im ersten Betriebsmodus sicherheitskritische Programme redundant von beiden Ausführungseinheiten und im zweiten Betriebsmodus nicht sicherheitskritische Programme abgearbeitet werden.

19. Verfahren nach Anspruch 18, dadurch gekennzeichnet, dass die sicherheitskritischen Programme redundant in den Ausführungseinheiten jeweils zugeordneten ersten Speicherbereichen abgelegt sind.

20. Verfahren nach Anspruch 18, dadurch gekennzeichnet, dass die nicht sicherheitskritischen Programme in einem einzigen zweiten Speicherbereich abgelegt sind und beide Ausführungseinheiten im zweiten Betriebsmodus nur auf den zweiten Speicherbereich zugreifen.

21. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass im ersten Betriebsmodus sicherheitskritische Programme redundant abgearbeitet werden und die dabei

entstehenden Zustände auf Übereinstimmung verglichen werden.

22. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass in dem ersten Betriebsmodus von den Ausführungseinheiten jeweils nur auf einen jeder Ausführungseinheit zugeordneten ersten Speicherbereich zugegriffen wird.

23. Verfahren nach Anspruch 16, mit wenigstens zwei getrennten Speicherbereichen, wobei in dem ersten Betriebsmodus beide Ausführungseinheiten nur auf einen beiden Ausführungseinheiten zugeordneten ersten Speicherbereich zugreifen.

24. Verfahren nach Anspruch 16 und 23, dadurch gekennzeichnet, dass die vorgegebene Speicheradresse als Triggeradresse im ersten Speicherbereich enthalten ist und die folgende Adresse auf die zugegriffen werden soll in dem zweiten Speicherbereich enthalten ist.

25. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass in dem zweiten Betriebsmodus von beiden Ausführungseinheiten nur auf einen, beiden Ausführungseinheiten zugeordneten zweiten Speicherbereich zugegriffen wird.

26. Verfahren nach Anspruch 16 und 25, dadurch gekennzeichnet, dass überwacht wird, dass die Auswertemittel im zweiten Betriebsmodus nur auf den zweiten Speicherbereich zugreifen.

27. Verfahren nach Anspruch 16 und 22 oder 23, dadurch gekennzeichnet, dass überwacht wird, dass die Auswertemittel im ersten Betriebsmodus nur auf den ersten Speicherbereich zugreifen.

28. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass eine Umschaltung von dem zweiten Betriebsmodus in den ersten Betriebsmodus durch eine Unterbrechungsanforderung erfolgt, wobei die Unterbrechungsanforderung durch eine Zeitbedingung oder eine Zustandsbedingung ausgelöst wird.

20.06.03 Sy/Ho

ROBERT BOSCH GMBH, 70442 Stuttgart

Verfahren zur Umschaltung zwischen wenigstens zwei Betriebsmodi einer Prozessoreinheit sowie entsprechende Prozessoreinheit

Zusammenfassung

Verfahren zur Umschaltung zwischen wenigstens zwei Betriebsmodi einer Prozessoreinheit mit wenigstens zwei Ausführungseinheiten dadurch gekennzeichnet, dass ein Wechsel von einem ersten Betriebsmodus in einen zweiten Betriebsmodus dadurch ausgelöst wird, dass durch die Prozessoreinheit auf eine vorgegebene Speicheradresse zugegriffen wird.

Figur 1

R306264

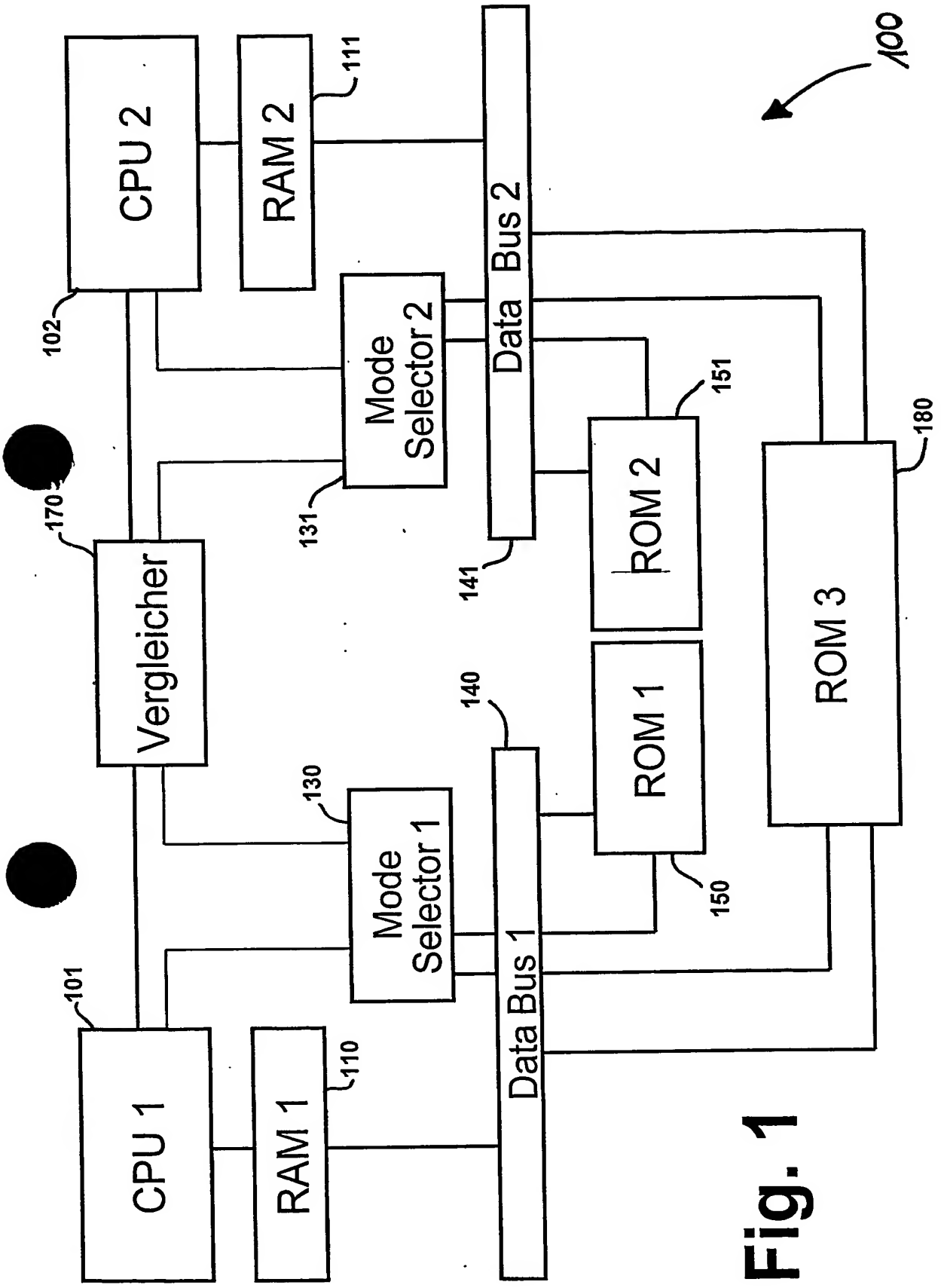

Fig. 1

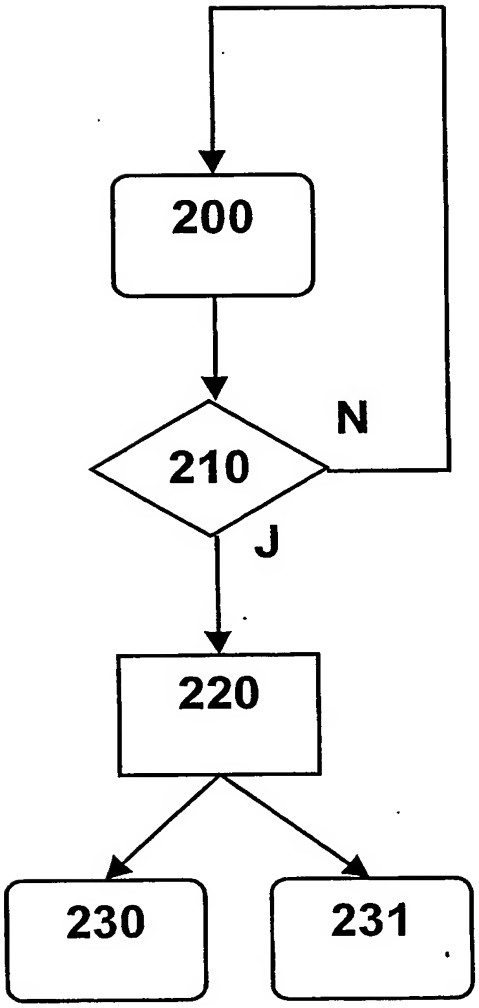

Fig. 2

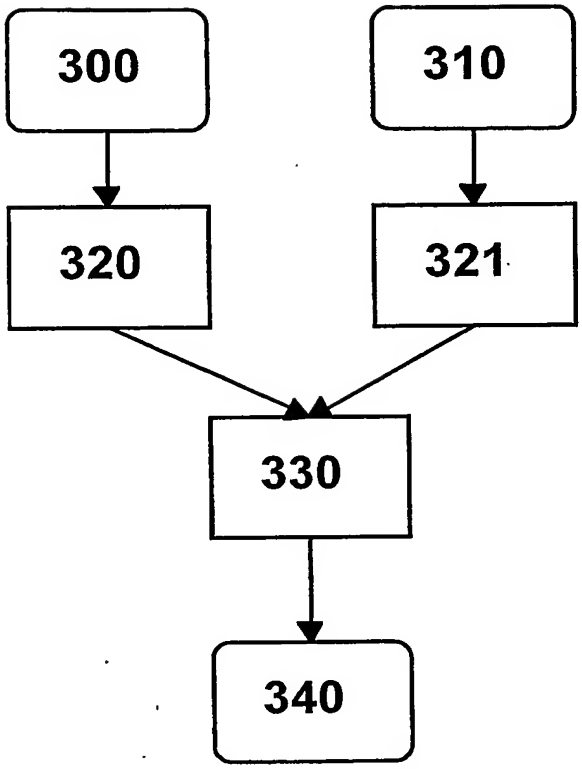

Fig. 3